

Original citation:

Dunne, P. E. (1984) Some results on replacement rules in monotone Boolean networks. University of Warwick. Department of Computer Science. (Department of Computer Science Research Report). (Unpublished) CS-RR-064

Permanent WRAP url:

<http://wrap.warwick.ac.uk/60764>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

A note on versions:

The version presented in WRAP is the published version or, version of record, and may be cited as it appears here. For more information, please contact the WRAP Team at: publications@warwick.ac.uk



<http://wrap.warwick.ac.uk/>

The University of Warwick

THEORY OF COMPUTATION

REPORT NO. **64**

SOME RESULTS ON REPLACEMENT RULES IN MONOTONE
BOOLEAN NETWORKS

by

Paul E Dunne

University of Warwick
Department of Computer Science
Coventry CV4 7AL
England

January 1984

Some Results On Replacement Rules In Monotone Boolean Networks

Paul. E. Dunne

Department Of Computer Science
University Of Warwick
Coventry CV4 7AL
Great Britain

1. Introduction

Replacement rules were introduced by Paterson [4] and Mehlhorn [3] and used to prove tight lower bounds on the monotone network complexity of boolean matrix multiplication. The results applied prove that in networks computing boolean matrix product, gates computing certain functions may be replaced by the constants 0 or 1 or by an input of the network. Applications of replacement rules to other functions have been made by Weiss [6] for boolean convolution and Dunne [2] for threshold functions.

In this paper we investigate the following problem:

(P1) Given a pair of boolean functions $f: \{0,1\}^n \rightarrow \{0,1\}$, $g: \{0,1\}^n \rightarrow \{0,1\}$ what are the monotone boolean functions h such that for any monotone network S computing f , containing a gate u which computes the function g , $S^{RES(u):=h}$ still computes f ?

We prove the following results:

R1) For any function f we derive closed form expressions for the maximal 0-replaceable and minimal 1-replaceable functions with respect to f .

R2) For any pair of functions f, g we determine closed form expressions for:

(i) $\min s$ such that g is replaceable by s in a network computing f

(ii) $\max s$ such that g is replaceable by s in a network computing f

R3) For any pair of functions f, g we determine closed form expressions for:

(i) $\min s$ such that s is replaceable by g in a network computing f

(ii) $\max s$ such that s is replaceable by g in a network computing f

Using (R2) we obtain a complete solution for (P1).

The remainder of this paper is organised as follows. Below we give basic definitions and the notation used. In Section(2) we derive (R1), (R2) and (R3) above. In Section(3) we extend our results to multiple-output functions and illustrate some applications. In Section(4) we prove the existence of "pseudo-complements" for all single-valued monotone boolean functions and characterise these.

Definition 1

A *monotone network* S is a directed acyclic graph with 2 distinguished sets of nodes: X (the *inputs* of S) is the set of nodes with in-degree 0. These nodes are labelled with members of the set $\{x_1, \dots, x_n\}$. G is the remaining set of nodes, which have in-degree 2 (the *gates* of S). Gates are labelled by \wedge or \vee (Boolean conjunction and disjunction).

□

Definition 2

If S is a monotone network and u is a node of S , $RES(u)$ is the boolean function recursively defined by:

$$RES(u) = \begin{cases} x_i & \text{if } u \text{ is input } x_i \text{ of } S \\ RES(u_1) \wedge RES(u_2) & \text{if } u \text{ is an } \wedge \text{ gate} \\ RES(u_1) \vee RES(u_2) & \text{if } u \text{ is an } \vee \text{ gate} \end{cases}$$

where u_1 and u_2 are the inputs of u if u is a gate. \square

Definition 3

$$f(X) \leq g(X) \Leftrightarrow \forall \alpha \in \{0,1\}^n f(\alpha)=1 \Rightarrow g(\alpha)=1$$

\square

Definition 4

A monom m is a function of the form:

$$m = x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_q} \quad x_{i_j} \in X$$

A monom m is an *implicant* of the monotone boolean function f if and only if

$m \leq f$. m is a *prime implicant* if:

- 1) m is an implicant of f
- 2) $\forall m'$ such that $m < m'$, m' is not an implicant of f

\square

Definition 5

A *clause* c is a function of the form:

$$c = x_{i_1} \vee x_{i_2} \vee \dots \vee x_{i_q} \quad x_{i_j} \in X$$

A clause c is an *implicand* of the monotone boolean function f if and only if

$f \leq c$. c is a *prime clause* if:

- 1) c is an implicand of f
- 2) $\nexists c'$ such that $c' < c$, c' is not an implicand of f .

□

Notation

$$PI(f) = \{ m \mid m \text{ is a prime implicant of } f \}$$

$$PC(f) = \{ c \mid c \text{ is a prime clause of } f \}$$

2. Results

Definition 6

Let $f: \{0,1\}^n \rightarrow \{0,1\}$, $g: \{0,1\}^n \rightarrow \{0,1\}$ and $h: \{0,1\}^n \rightarrow \{0,1\}$ be any monotone boolean functions.

g is h -replaceable with respect to f ($g \stackrel{f}{=} h$) iff:

$S|_{RES(u):=h}$ still computes f

for any monotone network S computing f which contains a node u with $RES(u)=g$ \square

The following result is the replacement rule due to Mehlhorn [3].

Lemma 1

$g \stackrel{f}{=} 0$ iff:

$\forall m \in PI(g) \quad \exists m'$ such that

$$m \wedge m' \in PI(f)$$

\square

An easy corollary of this is:

Lemma 2

$g \stackrel{f}{=} 1$ iff:

$$\forall h \quad g \wedge h \leq f \Rightarrow h \leq f$$

□

We shall now characterise the largest 0-replaceable and smallest 1-replaceable functions with respect to any function f . Although the results are implied by Theorem(3) below, we shall present these cases separately as the analysis is clearer. The characterisations use the representation of f as a conjunction of prime clauses (Conjunctive Normal Form) or as a disjunction of prime implicants (Disjunctive Normal Form).

Definition 7

Let f be a monotone boolean function over $\{x_1, \dots, x_n\}$. The *dual* of f (\bar{f}) is the monotone function:

$$\bar{f} = \neg (f(\neg x_1, \dots, \neg x_n))$$

where " \neg " denotes negation.

□

Definition 8

Let m be a monom, c be a clause and f be a monotone boolean function.

Then:

$$1) \quad \chi(m) = \vee \{x \mid m \leq x\}$$

$$2) \quad OC(f) = \bigwedge_{m \in PI(f)} \chi(m)$$

$$3) \quad \varphi(c) = \bigwedge \{x \mid x \leq c\}$$

$$4) \quad IC(f) = \bigvee_{c \in PC(f)} \varphi(c)$$

□

Theorem 1 (0,1-replacements)

(A) $OC(f)$ is the unique largest 0-replaceable function with respect to f . i.e

$OC(f) < g \Rightarrow g$ is not 0-replaceable w.r.t f .

(B) $IC(f)$ is the unique smallest 1-replaceable function with respect to f . i.e.

$IC(f) > g \Rightarrow g$ is not 1-replaceable w.r.t f .

Proof

Let:

$$Dross(f) = \bigvee \{ g \mid g \stackrel{f}{=} 0 \}$$

We shall show that:

$$OC(f) = Dross(f)$$

(i) $OC(f) \leq Dross(f)$

Suppose $m \leq OC(f)$, but that $m \not\leq Dross(f)$. Then there is some monom m' such that $m \wedge m' \in PI(f)$ and so m is a shortening of some prime implicant r of f . But:

$$m \leq OC(f) = \bigwedge_{p \in PI(f)} \chi(p) \Rightarrow m \leq \chi(r)$$

By monotonicity

But $\mathbf{m} \not\leq \chi(\mathbf{r})$ if \mathbf{m} is a shortening of \mathbf{r} . Contradiction.

(ii) $Dross(f) \leq OC(f)$

Let $\mathbf{m} \in PI(Dross(f))$, by Lemma(1) there does not exist \mathbf{m}' such that $\mathbf{m} \wedge \mathbf{m}' \in PI(f)$. Thus:

$$\forall \mathbf{r} \in PI(f) \quad \mathbf{m} \leq \chi(\mathbf{r})$$

$$\mathbf{m} \leq \bigwedge_{\mathbf{p} \in PI(f)} \chi(\mathbf{p}) \leq OC(f)$$

Thus:

$$OC(f) = Dross(f)$$

and (A) follows as $Dross(f)$ is by definition the largest 0-replaceable function with respect to f .

(B) It is easy to see that:

$$IC(f) = \overline{OC(f)}$$

Thus, by duality, $IC(f)$ is the unique minimal 1-replaceable function with respect to f .

□

We shall now consider non-constant replacements of the form $f := s$, and determine minimum and maximum solutions for these.

Definition 9

Let $\mathbf{M} = \{m_1, \dots, m_k\}$ be a set of monoms, and let f be a monotone boolean function. The *Prime-Implicant Extension* of \mathbf{M} with respect to f ($\mathbf{IE}_f(\mathbf{M})$) is defined to be:

$$\mathbf{IE}_f(\mathbf{M}) = \{ p \in \mathbf{PI}(f) \mid \exists m_i \in \mathbf{M} \text{ with } p \leq m_i \}$$

The *Prime-Clause Extension* of a set of clauses $\mathbf{C} = \{c_1, \dots, c_k\}$ with respect to f ($\mathbf{CE}_f(\mathbf{C})$) is given by:

$$\mathbf{CE}_f(\mathbf{C}) = \{ p \in \mathbf{PC}(f) \mid \exists c_i \in \mathbf{C} \text{ with } c_i \leq p \}$$

$$A(f, g) = \bigvee_{m \in \mathbf{IE}_f(\mathbf{PI}(g))} m$$

$$B(f, g) = \bigwedge_{c \in \mathbf{CE}_f(\mathbf{PC}(g))} c$$

□

Theorem 2

Let f, g be monotone boolean functions. Then:

- 1) $A(f, g)$ is the minimal function s such that $g \stackrel{f}{=} s$
- 2) $B(f, g)$ is the maximal s such that $g \stackrel{f}{=} s$

Note: Conventionally the empty monom (clause) is 1 (0).

Proof

- 1) Certainly g is $A(f, g)$ -replaceable when computing f , as by definition $\Pi_f(\Pi(g))$ is the set of all prime implicants of f to which g could be extended. So suppose some function s exists, also satisfying these requirements and that $A(f, g) \neq s$. There must be some prime implicant of $A(f, g)$, p say, which is not an implicant of s . Now:

$$p \in \Pi(f) \quad \text{and} \quad \exists m \in \Pi(g) \text{ such that } p \leq m$$

$$\text{So; } \Pi(g \wedge p) \cap \Pi(f) = \{p\}$$

$$\text{But; } \Pi(g \wedge ps) \cap \Pi(f) = \{\} \text{ as } p \not\leq s$$

Contradiction, as g is not replaceable by s when computing f .

Thus $A(f, g)$ is a minimal function. We now establish uniqueness. Suppose s_1, s_2 are distinct i.e. incomparable minimal functions. Then:

$$\begin{aligned} \Pi(g \wedge h) \cap \Pi(f) &\subset \Pi(g \wedge s_1 \wedge h) \cap \Pi(f) \\ &\subset \Pi(g \wedge s_1 \wedge s_2 \wedge h) \cap \Pi(f) \\ &\text{as } g \wedge s_1 \wedge h \leq f \end{aligned}$$

Thus $s_1 \wedge s_2 (\leq s_1, s_2)$ is also a suitable, but smaller function. Contradiction.

2) Duality

□

Corollary 2.1)

$g \stackrel{f}{=} h$ if and only if:

$$\vee \text{IE}_f(g) \leq h \leq \wedge \text{CE}_f(g)$$

□

Definition 10

$$\text{PI}_{\text{rem}}(f, g) = \text{PI}(f) - \text{IE}_f(\text{PI}(g))$$

$$\text{PC}_{\text{rem}}(f, g) = \text{PC}(f) - \text{CE}_f(\text{PC}(g))$$

$$E(f, g) = \bigwedge_{m \in \text{PI}_{\text{rem}}(f, g)} \chi(m)$$

$$D(f, g) = \bigvee_{c \in \text{PC}_{\text{rem}}(f, g)} \varphi(c)$$

□

Theorem 3

(A) $E(f, g)$ is the maximal s such that $s \stackrel{f}{=} g$.

(B) $D(f, g)$ is the minimal s such that $s \stackrel{f}{=} g$.

Proof

We need only prove (A) as (B) will follow by duality.

$$1) \quad E(f,g) \stackrel{f}{=} g$$

By Cor(2.1) we need only show:

$$A(f, E(f,g)) \leq g \leq E(f,g)$$

$$(i) \quad g \leq E(f,g)$$

Let $p \leq g$. Then by definition of $PI_{rem}(f,g)$:

$$\neg \exists m' \text{ such that } p \wedge m' \in PI_{rem}(f,g)$$

Thus:

$$\forall m \in PI_{rem}(f,g) \quad p \leq \chi(m)$$

By the definition of $E(f,g)$ this implies the result.

$$(ii) \quad A(f, E(f,g)) \leq g$$

Let: $p \in PI(A(f, E(f,g)))$. Now:

$$IE_f(PI(E(f,g))) \cap IE_f(PI_{rem}(f,g)) = \{\}$$

Thus either $p \in PI(f)$, in which case p is a lengthening of some prime implicant m of g or $p=0$. In both cases $p \leq g$.

$$2) \quad E(f,g) \text{ is maximal}$$

Suppose $u \not\leq E(f,g)$ and $u \stackrel{f}{=} g$. Then

$$\exists p \in PI(u) \text{ such that } p \not\leq E(f,g)$$

Thus: $E(f,g) \leq \chi(p)$ and therefore,

$$\exists r \in PI_{rem}(f,g) \text{ such that } \chi(r) \leq \chi(p)$$

So $r \leq p$. Thus:

$$u \wedge r = r \in PI(f)$$

$$g \wedge r \neq r \text{ (As } r \in PI_{rem}(f, g))$$

Thus u is not g -replaceable with respect to f . Contradiction. \square

Corollary 3.1)

$h \stackrel{f}{\equiv} g$ if and only if:

$$c \in PC_{rem}(f, g) \vee \varphi(c) \leq h \leq m \in PI_{rem}(f, g) \wedge \chi(m)$$

\square

Beynon [1] has considered a concept of "computational equivalence" within a different framework. g is said to be equivalent to h when computing f (

$g \stackrel{f}{\equiv} h$) if and only if $g \stackrel{f}{\equiv} h$ and $h \stackrel{f}{\equiv} g$. In this context Cor(2.1) and Cor(3.1)

yield:

Theorem 4

$g \stackrel{f}{\equiv} h$ iff

$$A(f, g) \vee D(f, g) \leq h \leq B(f, g) \wedge E(f, g)$$

Proof

Obvious

□

3. Multiple Output Functions

Let $F = \{f_1, \dots, f_m\}$ be any set of m monotone boolean functions over X

Theorem 5

$$OC(F) = \bigwedge_{i=1}^m OC(f_i)$$

$$IC(F) = \bigvee_{i=1}^m IC(f_i)$$

$$A(F, g) = \bigvee \mathbf{IE}_F(PI(g))$$

$$B(F, g) = \bigwedge \mathbf{CE}_F(PC(g))$$

$$E(F, g) = \bigwedge_{i=1}^m E(f_i, g)$$

$$D(F, g) = \bigvee_{i=1}^m D(f_i, g)$$

where;

$$\mathbf{IE}_F(M) = \{p \in \bigcup_{i=1}^m PI(f_i) \mid \exists m_i \geq p\}$$

$$\mathbf{CE}_F(C) = \{r \in \bigcup_{i=1}^m PC(f_i) \mid \exists c_i \leq r\}$$

Proof

Elementary

□

As an illustration we reprove the replacement rule due to Paterson [4] for Boolean Matrix Multiplication. Let:

$$BMP \{0,1\}^{2n^2} \rightarrow \{0,1\}^{n^2}$$

where each output c_{ij} is defined by:

$$c_{ij} = \bigvee_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} (x_{ik} \wedge y_{kj})$$

Lemma 3 (Paterson [4])

Let $BMP = \{c_{11}, \dots, c_{nn}\}$, where c_{ij} is as defined above. Let $1 \leq i, i' \leq n$ ($i \neq i'$) and $1 \leq j, j' \leq n$ ($j \neq j'$).

$$3.1) x_{ik} \vee x_{i'k} \stackrel{BMP}{=} 1$$

$$3.2) y_{kj} \vee y_{kj'} \stackrel{BMP}{=} 1$$

$$3.3) x_{ik} \vee y_{kj} \stackrel{BMP}{=} 1$$

Proof

$$\begin{aligned} IC(c_{ij}) &= \overline{OC(c_{ij})} \\ &= \overline{OC\left(\bigwedge_{1 \leq k \leq n} (x_{ik} \vee y_{kj})\right)} \\ &= \overline{\bigvee_{\substack{1 \leq p \leq n \\ 1 \leq q \leq n}} x_{pq} \vee \bigvee_{\substack{1 \leq r \leq n \\ 1 \leq s \leq n}} y_{rs} \vee c_{ij}} \\ &= \bigwedge x_{pq} y_{rs} \wedge \overline{c_{ij}} \end{aligned}$$

Thus:

$$IC(BMP) = \bigvee_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \left(\bigwedge x_{pq} y_{rs} \overline{c_{ij}} \right)$$

It is easy to see that for each of the function s in (3.1)-(3.3):

$$IC(BMP) \vee s = s \Rightarrow IC(BMP) \leq s$$

□

A k -slice function of f is a function of the form:

$$f \wedge T_k^P \vee T_{k+1}^P$$

The following is due to Wegener[5].

Lemma 4

If g is a k -slice function then:

$$\forall x_i \in X: x_i \stackrel{g}{=} | x_i \wedge T_k^P(X)$$

Proof

Easily derived from Theorem(2) above. □

Corollary

If g is a k -slice function then:

$$\forall x_i \in X: x_i \stackrel{g}{=} | x_i \vee T_{k+1}^P(X)$$

Proof

Duality.

□

4. Replacement Rules & Pseudo-Complements

Definition 11

Let f be a monotone boolean function over X . A *pseudo-complement* for x_i is a monotone boolean function h_i , such that in any $(\wedge, \vee, -)$ -network T computing f , in which negation is applied only to the inputs, any instance of $\neg x_i$, can be replaced by h_i and the resulting network will still compute f .

□

Theorem 6

\forall monotone f , h_i is a pseudo-complement for x_i if and only if:

$$f|_{x_i=0} \leq h_i \leq f|_{x_i=1}$$

Proof

Let f_0 denote the function computed by T after some instance, z say, of $\neg x_i$ is replaced by $f|_{x_i=0}$. Similarly let f_1 denote the function computed by T after this instance, z , is replaced by $f|_{x_i=1}$. Now since $f_0 \leq f_1$ it is sufficient to prove that:

$$f_1 \leq f \leq f_0$$

In terms of the instance z of $\neg x_i$, T computes:

$$g_{000} \vee x_i g_{100} \vee \neg x_i g_{010} \vee z g_{001} \vee \neg x_i z g_{011} \vee x_i z g_{101}$$

where the functions $g_{\alpha\beta\gamma}$ are such that:

1) $\forall \mathbf{m} \in \text{PI}(g_{\alpha\beta\gamma})$:

$$(x_i)^\alpha (-x_i)^\beta (z)^\gamma \wedge \mathbf{m}$$

is a monom computed at \mathbf{T} .

2) \mathbf{m} does not depend on x_i , $-x_i$ or z .

where:

$$(x)^\delta = \begin{cases} 1 & \text{if } \delta = 0 \\ x & \text{if } \delta = 1 \end{cases}$$

Clearly:

$$f = g_{000} \vee x_i g_{100} \vee -x_i (g_{010} \vee g_{001} \vee g_{011})$$

Now let $z := f^{x_i=0}$ so that $f := f_0$. We must prove $f \leq f_0$. We need only show:

$$-x_i g_{001} \vee -x_i g_{011} \leq f_0$$

However; $f^{x_i=0} \wedge g_{001} = g_{001}$ and $-x_i f^{x_i=0} g_{011} = -x_i g_{011}$ thus $f \leq f_0$.

Now consider the replacement $z := f^{x_i=1}$. We must show that $f_1 \leq f$. Similarly we need only prove:

$$f^{x_i=1} g_{001} \vee -x_i f^{x_i=1} g_{011} \vee x_i f^{x_i=1} g_{101} \leq f$$

But:

$$f^{x_i=1} \wedge g_{001} = g_{001} \leq f$$

$$-x_i \wedge f^{x_i=1} \wedge g_{011} \leq g_{011} \leq f$$

$$x_i \wedge f|_{x_i=1} \wedge g_{10i} \leq f$$

Thus $f_1 \leq f$, and the theorem follows. \square

Corollary 6.1)

Let $F = \{f_1, \dots, f_m\}$ be a set of m monotone boolean functions. Then h_i is a pseudo-complement for x_i if and only if:

$$\bigvee_{j=1}^m f_j|_{x_i=0} \leq h_i \leq \bigwedge_{j=1}^m f_j|_{x_i=1}$$

\square

We note that for sets of monotone boolean functions, in general the interval of Corollary(6.1) is not well-defined. However for special cases, such as slice functions, pseudo-complements exist. For slice functions Theorem(6) and Corollary(6.1) combined yield the results of Berkowitz (cited in [5]) for transforming combinational networks to monotone networks efficiently.

5. References

- [1] Beynon, M

Replaceability and computational equivalence in finite distributive lattices:
Theory Of Computation Report No.61, Univ. Of Warwick, March 1984.

- [2] Dunne, P.E.

A $2.5n$ Lower Bound On The Monotone Network Complexity Of T_3^F , Theory Of
Computation Report No.62, Univ Of Warwick, March 1984.

- [3] Mehlhorn, K. & Galil, Z.

Monotone Switching Networks and Boolean Matrix Product, Computing (16),
99-111, 1976

- [4] Paterson, M.S.

Complexity Of Monotone Networks For Boolean Matrix Product, Theoretical
Computer Science (1), 13-20, 1975

- [5] Wegener, I

On The Complexity Of Slice-Functions, Internal Report, Univ. Of Frankfurt,
July 1983

- [6] Weiss, J

A $n^{5/2}$ Lower Bound On The Boolean Convolution, Univ. Of Bielefeld, West
Germany, November 1982